REMARKS

Status of the Application:

Claims 1–56 are the claims of record of the application. Claims 1–3, 5–38 and 40–56 have been rejected and claims 4 and 39 have been objected to and would be allowable if written in independent form.

Amendment to the Specification and Abstract

Applicants have amended the Abstract as suggested by the Examiner to overcome an objection for use of "Disclosed herein."

Amendment to the Claims:

Applicants have amended the claims to overcome some objections in a manner suggested by the Examiner, and also to overcome rejections. Details of the substantive amendments are described below.

In particular, the claims have been amended to overcome the 35 USC 101 rejection, and further to add the feature that the wireless station that transmits the configuration message waits a settable time interval before wirelessly transmitting the configuration message, a feature that is not taught or suggested by any of the cited prior art.

Claim Objections

In paragraph 2 of the office action, claim 3, 4, 7, 12, 15, 16, 22, 25, 32, 33, 37–44, 45–48, 50–56 were objected to because of some informalities. The Examiner suggested changes that would overcome the objections, and Applicants thank the Examienr for these suggestions.

Applicants have amended the claims as suggested by the examiner in all cases but those in which the examiner objected to use of the indefinite article in reciting dependent claims.

With respect to claims 37–43, 45–48, and 50–56, each of claims 37–43, 45–48, and 50–56 recites "An apparatus " in line 1, and this recitation does indeed refer to an earlier claimed apparatus using, in each case, the term "as recited in claim" XX, where XX is a respective prior claim. However, because each claim of the set of claim is a ***separate***

invention, Applicants believe that use of the indefinite article "An" is appropriate. Using the definite article "The" would suggest the **same** apparatus. The Apparatus is not the same – there are additional features that are recited in the additional recitations.

Claim Rejections -35 USC § 101

In paragraph 4 of the office action, claims 20–35 were rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The Examiner suggested language to overcome this rejection, and Applicants that Examiner for this suggestion. Claims 20–35 have been amended as suggested by the Examiner. The claims as amended therefore meet 35 USC 101.

Claim Rejections -35 USC § 102

In paragraph 6 of the office action, claims 1, 6, 7, 11, 12, 14, 16, 20, 24, 25,28,29,31, 33, 36, 40, 41, 49, 50, 52 and 54 were rejected under 35 U.S.C. 102(b) as being anticipated by Havarinen et al (US 2002/0012433 Al).

The Application in the pertinent part

The Application describes methods and systems for automatic configuration of devices in a wireless network. The common users using wireless devices for establishing a WLAN in a small office or home office (SOHO) generally find configuring these wireless devices complicated and cumbersome. For a client station or an access point (AP) to function on WLAN, it is required that Configuration parameters be set. These parameters include parameters about protocol and transmission mechanism to use, a station's host address, available services on the network, etc. There are existing methods that can provide configuration parameters to a client station, even with limited or no user intervention. However, security parameters such as security keys need to be configured manually. It is the security key that is difficult for SOHO to configure on wireless stations. This security key also needs to be transmitted from one wireless station to another wireless station. The security key should not be communicated openly such that it can be eavesdropped, lest the security mechanism be rendered ineffectual. But it is the step of transferring the security key from one wireless station to another that many home or SOHO users find unacceptable-too difficult and/or too cumbersome-to perform regularly. As a consequence, many home and SOHO users today do not enable wireless security

mechanisms, leaving their WLANs particularly vulnerable to eavesdropping and unauthorized use.

The Application describes a method and apparatus that provide configuration parameters to wireless stations on a WLAN with little or no user-intervention.

In the configuration sequence, the AP transmits a discovery message such that client stations can respond with a configuration request message if they are able to receive and decode the discovery message. If the AP receives no configuration request messages within a pre fixed time interval, then the AP-implemented configuration sequence ends. On the other hand, the AP processes each client station that responds in the time interval. The AP carries out a set of steps for each of the responding client stations. It processes the client station by generating a configuration data message for the client station, transmitting the configuration data message to the client station and waiting within a settable time interval for a configuration acknowledgement message from the client station. If the AP receives no configuration acknowledgement message from the client station within the set time interval, then the AP reprocesses the client station until either a configuration acknowledgement message has been received, or a maximum number of reprocessing steps has occurred.

On a client station of a configuration sequence corresponding to the AP-implemented sequence, the client station is in a state in which it waits for a discovery message from an AP. As a result of receiving a discovery message from a particular AP, the client station waits a random backoff time interval to minimize the occurrence of configuration request message collisions from other client stations, transmits a configuration request message to the AP and waits for up to a settable time interval for a configuration data message from the AP.

If it determines that it received no configuration request message, then the client station-implemented configuration sequence ends. If a configuration data message has been received, then the client station extracts configuration parameters from the configuration data message, applies the configuration parameters and transmits a configuration acknowledgement message to the particular AP. Once the AP configures the client station(s), the configuration sequence in the AP ends.

The Application further describes the mechanism to reduce the probability of inadvertent reception of configuration parameters transmitted by an AP to a client station. This is achieved in one embodiment by limiting the output RF power level of transmitted

signals (RF security.). A wireless network transmitter coupled to an antenna cannot directly control which wireless receivers are able to receive its transmitted signals. Any compatible wireless network receiver with sufficient sensitivity and within sufficient range of the transmitter will be able to receive signals transmitted by the wireless transmitter. By reducing the power of the transmitting signals, the range of reception of the signals, that is, the region in which a wireless station can receive and decode the signals, is limited. This can be done using a variable attenuator coupled between the antenna and a wireless transceiver or by electronically reducing the size of the signal prior to power amplification in the transmit part of the transceiver at the AP.

FIG. 3 shows a BSS in a WLAN with three zones defined by an AP, a minimum broadcast distance, and a maximum broadcast distance. Inside the minimum broadcast distance, Zone I, a client station can receive and decode signals transmitted by the AP. Outside the maximum broadcast distance, Zone III, a client station is unable to receive and decode signals transmitted by the AP. Between Zone I and Zone III is Zone II, wherein a client station may or may not be able to receive and decode signals transmitted by the AP.

RF security can also be provided by setting the AP's output RF power level used during a configuration sequence to a relatively low power level, thus reducing the range of reception. The method is called "low power RF security". Users that are authorized to receive configuration parameters can move their client stations close to the AP, into Zone I, before beginning the configuration sequence. Thus, the unauthorized client stations, those further away from the AP as in Zone III, have a reduced probability of receiving and decoding configuration parameters transmitted by the AP during a configuration sequence.

Another method that provides RF security includes setting the AP's output power level to a very low output RF power level, then stepping up the output RF power level until any client stations respond. This method is called "stepped RF security". Thus, those client stations that are close to the AP become configured, while those further away are unable to receive configuration parameters transmitted during a configuration sequence.

FIG. 4 describes a flowchart of the configuration sequence in an AP that includes the stepped RF security method.

1. AP sets its output RF power level to a settable first RF power level.

2. AP transmits a discovery message such that an appropriately equipped client station that receives the discovery message will respond with a configuration request message.

3. AP waits for a settable time interval for configuration request messages. If it receives no configuration request messages within the preset time interval, then it increases the output RF power level by a settable step size. If the output RF power level is not greater than a settable maximum output RF power level, it repeats the above sequence of steps.

4. If one or more configuration request messages are received by the AP within the preset time interval, the AP follows the configuring steps. Once the AP configures the client station(s) or the maximum power level is reached, the configuration sequence in the AP ends.

The Application further defines a protocol, called the One Touch Configuration (OTC) protocol, to implement a configuration sequence in a WLAN. The OTC protocol defines an OTC packet, embedded in an 802.11 sub network access protocol (SNAP) packet as per the IEEE 802.2 SNAP specification. The OTC packets have an OTC length field, a message type field, a session token field, and optionally some packets, called "type-length-value" (TLV) packets because each includes a type, a length, and a value field that can be any length. The OTC length field is a 2-byte field that refers to the length in bytes of the entire OTC packet, and the OTC type field is a 2-byte field that refers to the type of packet. The session token field is a 2-byte field used to differentiate sessions of the OTC protocol.

Further, a TLV packet has a TLV type field, a TLV length field and a TLV data field. The TLV type field is a 2-byte field that refers to the type of packet.

FIG. 7 as in the Application shows a message-flow diagram of a configuration sequence of an AP and two client stations using the OTC protocol and stepped RF security.

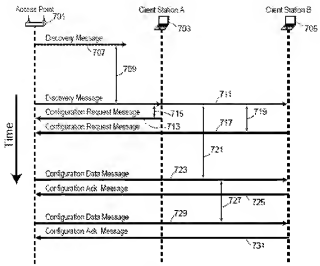

FIG. 7

The Application further describes a method for selecting which client stations are to be configured. It has two selection modes for a client station - the automatic client selection mode directs a client station to always respond to discovery messages, and to always configure itself upon reception of a valid configuration data message. In this mode, a client station is configured automatically by simply moving a client station into an automatic configuration zone. The other mode, the manual client selection mode is defined as selectively determining whether or not the client station is to be configured by either a user-settable parameter or a user interface. This mode enables a client station to be selectively configured based on user's input.

Summary of the relevant portions of Reference (Havarinen et al. US 2002/0012433 Al).

Havarinen describes a method for authenticating a mobile node to a packet data network, in which a shared secret for both the mobile node and the packet data network is arranged by using a shared secret of the mobile node and a telecommunications network authentication center.

Applicants have amended the claims to add a feature not taught in any of the cited prior art.

The Application at Page 4, paragraph [0026] describes that –

The AP starts by transmitting a discovery message in a step 103 such that client stations can respond with a configuration request message if they are able to receive and decode the discovery message. The AP waits for a settable time interval for one or more configuration request messages in a step 105. If the AP in a step 107 determines that it received no configuration request messages within the time interval of step 105, then the AP-implemented configuration sequence ends.

Havarinen does not disclose the concept of settable time interval. Haverinen describes that during shared session key exchange procedure, the MT sends a Network Access Identifier and a protection code generated by the MT to the FAAA. The FAAA sends an initial identification message containing the IMSI or NAI of the MT, and the protection code to the HAAA. The HAAA retrieves n GSM triplets and computes a shared session key for the MT. The HAAA also computes a cryptographic checksum to verify that the n codes really originate during the same authentication session because the MT_RAND changes from one authentication session to another.

The claims have been amended to include the feature of the settable time interval to each independent claim. Without commenting on the merits of the rejection, Applicants assert that there is no step in Avarinen of "waiting for a settable time interval to wirelessly receive a configuration request message from a second wireless station within the settable time interval" as in amended claim 1.

For example, Havarinen fails to disclose that FAAA waits for a settable time interval within which to receive Network Access Identifier and protection code from MT.

Hence claim 1 is now allowable over the cited prior art. Similarly, the other claims rejected under 35 USC 102 over Havarinen have been amended to recite a similar feature, so that such claims are also believed allowable.

Claim Rejections -35 USC § 103

In paragraph 9 of the office action claims 2, 3, 5, 13, 21, 22, 30, 37, 38, 44, 47, 48 and 51 were rejected under 35 U.S.C. 103(a) as being unpatentable over Havarinen et al (US 2002/0012433 Al, hereinafter "Havarinen"), in view of Tada et al (US 7,184,707 B2, hereinafter "Tada").

Summary of the relevant portions of Reference (Tada et al US 7,184,707 B2).

Tada describes a communication device and a method for controlling a communication device that can load or unload service information at appropriate timings by flexibly designating discriminating conditions of connection or disconnection of a link. When peripheral devices or extension cards are connected to a personal computer (PC), the PC is loaded with suitable driver software for the respective devices so that it may recognize hardware information for the additional devices. Recently, radio communication techniques such as "Bluetooth" or Home RF are being used in coupling. Similar to Bluetooth, Home RF is also a radio communication standard for a home application. Home RF uses the same ISM band of 2.4 GHz as a carrier frequency and communicates through a maximum data transmission speed of 1.6 Mbps in a service area covering a distance from 50 m to 100 m.

Applicants have amended the claims to add a feature not taught in any of the cited prior art.

In Paragrpah [0028], the Application states that

> *FIG. 2 shows a flowchart in a client station of a configuration sequence embodiment corresponding to the AP-implemented sequence of FIG. 1. In a step 201, the client station is typically in a state in which it waits for a discovery message from an AP. As a result of receiving a discovery message from a particular AP, the client station waits a random backoff time interval in a step 203 to minimize the occurrence of configuration request message collisions from other client stations, transmits a configuration request message to the AP in a step 205, and waits for up to a settable time interval for a configuration data message from the AP in a step 207.*

Claim 2 has been amended to recite that the first wireless station wirelessly transmits a discovery message, that the configuration request message wirelessly received at the first wireless station is as a result of the second wireless station responding to receiving the discovery message, e.g., within the settable time interval, and that the ***transmitting of the configuration message is after waiting for a backoff time interval***.

Haverinen does not disclose wirelessly transmitting a discovery message by a first wireless station. Rather, Haverinen describes that MT directly sends the Network Access Identifier and the protection code to the FAAA. This implies that FAAA does not

send a discovery message to the MT to begin with. Hence, Haverinen does not disclose **wirelessly transmitting a discovery message by a first wireless station.** The Application on the other hand on Page 10, paragraph [0051]-[0052] describes **that the AP begins with sending the discovery message so that an appropriately equipped client station would respond to the discovery message within a settable interval of time**. Haverinen fails to describe the discovery message as well as the settable interval of time.

Tada describes that the PC 1 transmits a message in response to the station discovery message of the target node. However, this happens in waiting mode which is different from the station discovery mode. However, the Application does not describe different modes for discovery message transmission and response to the transmission. In the Application, this happens sequentially irrespective of the mode of operation. Further, this response is time bound i.e. after receiving a discovery message from a particular AP, the client station waits **a random backoff time interval** to minimize the occurrence of configuration request message collisions from other client stations and then transmits a configuration request message to the AP. However, Tada fails to explain any such time interval.

Thus, claim 2 is believed allowable over Havarinen in view of Tada.

Similarly, the other cited claims rejected under 35 USC 103 over Havarinen in view of Tada either depend on this claim 2, or have had added similar limitations not taught by the combination of Havarinen in view of Tada.

Already Allowable Subject Matter

In paragraph 14 of the office action, it was stated that claim 4 and 39 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

For these reasons, and in view of the above amendment, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Conclusion

The Applicants believe all of Examiner's rejections have been overcome with respect to all remaining claims (as amended), and that the remaining claims are allowable. Action to that end is respectfully requested.

If the Examiner has any questions or comments that would advance the prosecution and allowance of this application, an email message to the undersigned at dov@inventek.com, or a telephone call to the undersigned at +1-510-547-3378 is requested.

Respectfully Submitted,

October 12, 2007 /Dov Rosenfeld/ #38687
Date Dov Rosenfeld, Reg. No. 38687

Address for correspondence:
Dov Rosenfeld
5507 College Avenue, Suite 2,
Oakland, CA 94618
Tel. 510-547-3378
Fax: +1-510-291-2985
Email: dov@inventek.com